TS

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/536,033	03/27/2000	Mariusz H. Jakubowski	MS1-515US	4016

22801 7590 12/23/2003

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
TRAN, TONGOC	
ART UNIT	PAPER NUMBER
2134	6

DATE MAILED: 12/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

TS

Office Action Summary	Application No. 09/536,033	Applicant(s) JAKUBOWSKI ET AL.
	Examiner Tongoc Tran	Art Unit 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-36 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-36 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) □ The translation of the foreign language provisional application has been received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5.

4) □ Interview Summary (PTO-413) Paper No(s). _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

1. This office action is in response to applicants' application serial no. 09/536033 filed on 3/27/2000.

Claim Objections

2. Claims 1, 4, 6,8,13,16, 21, 23, 25, 26, 27, 32, 33 and 35 are objected to because of the following informalities:

the phrase "digital good" appears to be inconsistent with the phrase "digital goods" in the specification. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 8,12 and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Yorke-Smith (U.S. Patent No. 5,548,648).

In respect to claim 8, Yorke-Smith discloses a method comprising:

segmenting a digital goods into a plurality of segments (see col. 3, lines 25-27).

selecting multiple segments from the plurality of segments (see col. 1, lines 53-55); and transforming the selected segments according to different protection techniques to produce a protected digital goods having a composite of variously protected segment (see col. 1, lines 58-67).

In respect to claim 12, Yorke-Smith discloses a method as recited in claim 8, wherein the transforming comprises:

Augmenting at least one segment using a certain protection technique (see col. 1, lines 48-65); and inserting a checkpoint, which may be used to evaluate a validity of the augmented segment, within the protected digital goods but outside of the augmented segment being evaluated (see col. 3, lines 25-42).

In respect to claim 17, the claim limitation is a computer-readable medium claim which is substantially similar to method claim 8 and therefore the same rejection applied.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Sung et al. (U.S. Patent No. 5,768,372 hereinafter Sung).

In respect to claim 1, Leppek discloses a method comprising:

receiving an original digital goods (see col. 2, lines 1-5) ; and

applying various forms of protection to the original digital goods to produce a protected digital goods (see col. 2, lines 14-38).

Leppek does not explicitly discloses applying randomly various forms of protection. However, Sung discloses randomly selects which of the encryption to use (see col. 6, lines 32-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Leppek for applying various forms of protection with Sung's teaching of selecting encryption randomly for a more secure data protection because a person attempting to copy the programming data would not be able to know which encryption is being used even if all the potential encryptions is known (see Sung, col. 3, lines 14-20).

In respect to claim 2, Leppek and Sung disclose a method as recited in claim 1, wherein the randomly applying comprises pseudo randomly applying the various forms of protection according to pseudo random techniques (see Sung, col. 4, lines 20-30).

In respect to claim 3, Leppek and Sung disclose a method as recited in claim 1, wherein the applying comprises randomly selecting the forms of protection from a set of available forms of protection (see Sung, col. 6, lines 32-40).

In respect to claim 4, Leppek and Sung discloses a method as recited in claim 1, wherein the applying comprises applying the various forms of protection to randomly selected portions of the original digital goods (see Sung, 3, lines 14-20).

In respect to claim 5, Leppek and Sung disclose a method as recited in claim 1. Both Leppek and Sunk discloses plurality of encryption tools but do not explicitly discloses wherein the various forms of protection are selected from a group of protection tools comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering, obfuscated function execution, encryption/decryption, probabilistic checking, Boolean check obfuscation, in-lining, reseeding pseudo random number generators with tune varying inputs, anti-disassembly methods, varying execution paths between runs, anti-debugging methods, and time/space separation between tamper detection and response. However, these various form of protection tools are old and well known. Therefore, it would have been obvious to one of ordinary skill in the art to implement the encryption system taught by Leppek and Sung with various protective tools for a more secure data protection because the more potential tools is used the more difficult it is for data to be tampered with.

In respect to claim 6, Leppek and Sung disclose method as recited in claim 1. Leppek and Sung do not explicitly disclose wherein the applying comprises applying a form of protection in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, performing checksum on data packet is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption system of Leppek and Sung with checksum to ensure transmitted data has not been tampered during the transmission.

In respect to claim 7, the claim limitation is a computer-readable medium claim which is substantially similar to method claim 1 and therefore the same rejection applied.

7. Claims 9 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648).

In respect to claim 9, Yorke-Smith discloses a method as recited in claim 8. Yorke-Smith does not explicitly discloses wherein at least two of the segments overlap one another. However, redundant packets sent over the network is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with data segments overlapping one another in an event that data is lost due to other interference.

In respect to claim 15, Yorke-Smith discloses a method as recited in claim 8. Yorke-Smith disclose using plurality of encryption tools but do not explicitly discloses wherein the various forms of protection are selected from a group of protection tools comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering, obfuscated function execution, encryption/decryption, probabilistic checking, Boolean check obfuscation, in-lining, reseeding pseudo random number generators with tune varying inputs, anti-disassembly methods, varying execution paths between runs, anti-debugging methods, and time/space separation between tamper detection and response. However, these various form of protection tools are old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith's encryption system with these specific protective tools because the more protective tools is used the harder it is to for the data to be tampered with.

In respect to claim 16, Yorke-Smith discloses method as recited in claim 8. Yorke-Smith do not explicitly disclose wherein the applying comprises applying a form of protection in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, performing checksum on data packet is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of Yorke-Smith's encryption system with checksum to ensure transmitted data has not been tampered during the transmission.

8. Claims 10-11, 23-26 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Sung et al. (U.S. Patent No. 5,768,372).

In respect to claim 10, York-Smith does not disclose but Sung discloses explicitly disclose a method as recited in claim 8, wherein the selecting comprises randomly selecting the segments (see col. 3, lines 1-20). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of randomly selecting the segments for a more secure data transmission because even if all the potential encryptions is known, one has to know which encryption is associated with a particular encryption selection data (see Sung, col. 3, lines 16-20).

In respect to claim 11, York-Smith does not explicitly disclose but Sung discloses a method as recited in claim 8, wherein the transforming comprises transforming the selected segments according to randomly chosen protection techniques (see Sung, col. 1-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because in order for a person to know which encryption from among all the available encryptions is associated with a particular encryption selection data (see Sung, col. 3, lines 15-20).

In respect to claim 23 York-Smith discloses a production system, comprising:

a memory to store an original digital goods (see col. 1, 1-10 and lines 48-52); and a production server equipped with a set of multiple protection tools that may be used to augment the original digital goods for protection purposes (see col. 1, lines 4-10 and col. 48-52), the production server being configured to parse the original digital goods (see col. 3, lines 25-27).

Furthermore, Yorke-Smith does not but Sung discloses apply protection tools selected from the set of protection tools to various portions of the original digital goods in a random manner to produce a protected digital goods having a composite of variously protected portions (see Sung, col. 3, lines 1-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because in order for a person to know which encryption from among all the available encryptions is associated with a particular encryption selection data (Sung, col. 3, lines 15-20).

In respect to claim 24, Yorke-Smith and Sung disclose a method as recited in claim 23. Yorke-Smith and Sung discloses using plurality of protective tools but do not explicitly discloses wherein the augmenting comprises applying a protection technique selected from a group of protection techniques comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering, obfuscated function execution, encryption/decryption, probabilistic; checking, Boolean check obfuscation, inlining, reseeding pseudo random number generators with time varying inputs, anti-disassembly methods, varying execution paths between runs, anti-debugging methods, and time/space separation between tamper detection and response. However, these various form of protection tools are old and well known. Therefore, it would have been obvious to one of ordinary skill in the art to implement the encryption system taught by Yorke-Smith and sung with various protective tools for a more secure data protection because the more potential tools is used the more difficult it is for data to be tampered with.

In respect to claim 25, Yorke-Smith and Sung do not disclose a method as recited in claim 23 wherein the applying comprises applying a form of protection in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, performing checksum on data packet is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption system of Yorke-Smith and Sung with checksum to ensure transmitted data has not been tampered during the transmission.

In respect to claim 26, Yorke-Smith and Sung disclose a production system as recited in claim 23, wherein the production server has a pseudo random generator to introduce randomness into the application of the protection tools to various portions of the original digital goods (see Sung, col. 4, lines 20-30).

In respect to claim 32, Yorke-Smith discloses a client-server system, comprising: a production server to apply various forms of protection to a digital goods to produce a protected digital goods (see col. 1, lines 48-67); and a client to store and execute the protected digital goods the client being configured to evaluate the protected digital goods (see col. 1, lines 1-10, col. 3, lines 5-12 and col. 5, lines 23-25).

Yorke-Smith does not disclose but Sung discloses randomly applying various forms of protection to a digital goods (see Sung, col. 6, lines 31-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because a person attempting to copy the programming data would not be able to know which encryption is being used even if all the potential encryptions is known (see Sung, col. 3, lines 14-20).

9. Claims 13-14, 18-22, 27-28, 31, 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) in view of Gutowitz (U.S. Patent No. 5,365,589).

In respect to claim 13, Yorke-Smith discloses a method as recited in claim 8. Yorke-Smith does not explicitly discloses but Gutowitz discloses comprising receiving quantitative parameters indicative of how much the protected digital goods should be altered (see col. 35, lines 39-67, partial encryption). It would have been obvious to one of ordinary skill in the art to combine the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Gutowitz's teaching of partially encrypting digital data so that it enables information of different levels of security and/or destined for different uses to encrypted into the same ciphertext (see Gutowitz, col. 35, lines 64-66).

In respect to claim 14, Yorke-Smith and Gutowitz further discloses a method as recited in claim 13, wherein the transforming is performed to satisfy the quantitative parameter (see Gutowitz, col. 35, lines 39-67).

In respect to claim 18, Yorke-Smith discloses a method comprising:

parsing the software product into code sections segments (see col. 3, lines 25-27);

selecting at least one code section (see col. 1, lines 53-55); augmenting the selected code section to add protection qualities (see col. 1, lines 58-67);

repeating the selecting and the augmenting for different code sections until the desired quantity of protection has been applied (see col. 1, lines 48-67).

Yorke-Smith does not explicitly discloses establishing parameters prescribing a desired quantity of protection to be applied to a software product and augmenting the selected code section to add protection qualities (partially encrypting code section). However, Gutowitz discloses partially encrypting image file (see col. 35, lines 39-67). It would have been obvious to one of ordinary skill in the art to combine the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Gutowitz's teaching of partially encrypting digital data so that it enables information of different levels of security and/or destined for different uses to encrypted into the same ciphertext (see Gutowitz, col. 35, lines 64-66).

In respect to claim 19, Yorke-Smith and Gutowitz disclose a method as recited in claim 18. York-Smith does not explicitly discloses wherein the establishing comprises enabling a user to enter the parameters. However, allowing user to manually entering data is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith's encryption system that allow the user to enter the parameters for the benefit of having user to decide what program data to be encrypted instead of the software to do the task.

In respect to claim 20, Yorke-Smith and Gutowitz disclose a method as recited in claim 18. Yorke-Smith and Gutowitz do not explicitly disclose wherein the augmenting comprises applying a protection technique selected from a group of protection techniques comprising code integrity verification, acyclic code integrity verification, cyclic code integrity verification, secret key scattering, obfuscated function execution, encryption/decryption, probabilistic; checking, Boolean check obfuscation, in lining, reseeding pseudo random number generators with time varying inputs, anti disassembly methods, varying execution paths between runs, anti-debugging methods, and time/space separation between tamper detection and response. However, these various form of protection tools are old and well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption system taught by Yorke-Smith and Gutowitz with these specific protective tools because the more protective tools is used the harder it is to for the data to be tampered with.

In respect to claim 21, Yorke-Smith and Gutowitz do not disclose a method as recited in claim 18, wherein the augmenting comprises applying a protection technique in which a checksum can be computed on a set of bytes of the digital goods without actually reading the bytes. However, performing checksum on data packet is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Yorke-Smith and Gutowitz's encryption system with checksum to ensure transmitted data has not been tampered during the transmission.

In respect to claim 22, the claim limitation is a computer-readable medium comprising computer-readable claim which is substantially similar to method claim 18 and therefore the same rejection applied.

In respect to claim 27, the claim limitation is a system claim which is substantially similar to method claim 18 and therefore the same rejection applied.

In respect to claim 28, the claim limitation is a system claim which is substantially similar to method claim 20 and therefore the same rejection applied.

In respect to claim 31, Yorke-Smith and Gutowitz disclose an obfuscation system as recited in claim 27, further comprising a quantitative unit to specify a quantity of protection qualities to be added to the digital goods (see Gutowitz, col. 35, lines 39-63).

In respect to claim 33, the claim limitation is a computer-readable media claim which is substantially similar to method claim 18 and therefore the same rejection applied.

In respect to claim 36, the claim limitation is a computer-readable media claim which is substantially similar to the method claim 20 and therefore the same rejection applied.

10. Claims 29-30 and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yorke-Smith (U.S. Patent No. 5,548,648) and Gutowitz (U.S. Patent No. 5,365,589) and further in view of Sung et al. (U.S. Patent No. 5,768,372).

In respect to claim 29 and 30, Yorke-Smith and Gutowitz do not disclose a obfuscation system as recited in claim 27, wherein the target segment selector comprises a pseudo random generator to enable random selection of the segment. However, Sung discloses using a pseudo random generator to enable random selection of segment and protection tool (see Sung, col. 3, lines 4-20 and col. 4, lines 20-30). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's and Gutowitz's encryption method for encrypting data into a plurality of controlled and data blocks with

Sung's teaching of selecting encryption by using pseudo random generator for a more secure data protection because in order for a person to know which encryption from among all the available encryptions is associated with a particular encryption selection data (Sung, col. 3, lines 15-20).

In respect to claim 34, Yorke-Smith and Gutowitz discloses one or more computer-readable media as recited in claim 33. Yorke-Smith and Gutowitz do not disclose but Sung discloses comprising computer-executable instructions to randomly select the protection, tools from a set of available protection tools (see Sung, col. 6, lines 32-40 and). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because a person attempting to copy the programming data would not be able to know which encryption is being used even if all the potential encryptions is known (see Sung, col. 3, lines 14-20).

In respect to claim 35, Yorke-Smith and Gutowitz disclose one or more computer-readable media as recited in claim 33. Yorke-Smith and Gutowitz do not discloses but Sun discloses comprising computer-executable instructions to apply the protection tools to randomly selected portions of the original digital goods (see Sung, col. 3, lines 1-20 and col. 6, lines 32-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of Yorke-Smith's and Gutowitz's encryption method for encrypting data into a plurality of controlled and data blocks with Sung's teaching of selecting encryption randomly for a more secure data protection because a person attempting to copy the programming data would not be able to know which encryption is being used even if all the potential encryptions is known (see Sung, col. 3, lines 14-20).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Sung et al. disclose a method and apparatus for securing programming data of programmable logic device.

-Allen discloses a method and system for ensuring royalty payment for data delivered over the network.

-Fahlman et al. Disclose a method for transforming message containing sensitive information.

-Marchant discloses a security apparatus for data transmission with dynamic random encryption.

-O'Brien discloses digital audio telephony over IP network compression.

-Tseng et al. Disclose facsmile message encryption system.

-Bye stream selective encryption/decryption device.

-Cryptographic communication system.

-Barrett et al. discloses an automatic encryption selector.

-Hall discloses an ADP security device for labeled data.

-Milsted et al. Discloses a method and apparatus to create encoded digital content.

Jandel discloses a method and device for encryption of images.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-9600.

Examiner Tongoc Tran
AU: 2134

TT
November 26, 2003

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134